AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph [0002] beginning on page 1, as follows:

[0002] As a copy protection measure for a digital broadcast program, a control signal "Copy Once", which indicates recording is permitted only once, is attached to the digital broadcast program, and the digital broadcast program with this "Copy Once" control signal is encrypted and broadcast. Such a digital broadcast program accompanied by the "Copy Once" control signal can be recorded using a recording/reproduction device that is compatible with CPRM (Content Protection for Recordable Media). The recorded digital broadcast program cannot be copied to another device, and can only be moved to another compatible device.

Patent document 1: Japanese Patent Application Publication No. 2003-228522.

Non-patent document 1: Shinichi Ikeno & Kenji Koyama *Modern Cryptosystem [Gendai Angouriron]*, I.E.I.C.E.

Non-patent document 2: Eiji Okamoto *Introduction to Theory of Cryptography [Angou Riron Nyumon]*~~*Introduction to Modern Encryption [Gendai Angou Nyumon]*~~, Kyoritsu Shuppan.

Please amend the paragraph [0005] beginning on page 3, as follows:

[0005] The stated aim can be achieved by a terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, including: a storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content; a decryption unit operable to decrypt the first encrypted content using the device key, to generate the content; a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content; an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content; ~~and~~ a write unit operable to move the medium key and the second encrypted content to the portable medium, and read the device key from the storage unit and write the read device key to the portable medium; and a key deletion unit operable to delete the device key from the storage unit.

Please amend the paragraph [0036] beginning on page 17, as follows:

[0036] FIG. 1 shows a construction of a content protection system 1.

FIG. 2 is a functional block diagram showing a functional construction of a

recording/reproduction device 10.

FIG. 3 shows information stored in a storage unit 104.

FIG. 4 shows specific examples of a title list output on a monitor 12.

FIG. 5 is a functional block diagram showing a functional construction of a portable medium 14.

FIG. 6 is a functional block diagram showing a functional construction of a mobile phone 15.

FIG. 7 is a flowchart showing an overall operation of the content protection system 1.

FIG. 8 is a flowchart showing an operation of moving content from the recording/reproduction device 10 to the portable medium 14.

FIG. 9 shows data held in the recording/reproduction device 10 and the portable medium 14, in a process of moving content from the recording/reproduction device 10 to the portable medium 14.

FIG. 10 is a flowchart showing an operation of moving content from the portable medium 14 to the recording/reproduction device 10.

FIG. 11 shows data held in the recording/reproduction device 10 and the portable medium 14, in a process of moving content from the portable medium 14 to the recording/reproduction device 10.

FIG. 12 shows a construction of a content protection system 1a.

FIG. 13 is a functional block diagram showing a functional construction of a PC 16.

FIG. 14 is a flowchart showing an overall operation of the content protection system 1a.

FIG. 15 is a flowchart showing an operation of moving content from the portable medium 14 to the PC 16, continuing to FIG. 16.

FIG. 16 is a flowchart showing the operation of moving content from the portable medium 14 to the PC 16, continuing from FIG. 15.

FIG. 17 shows a construction of a content protection system 2 and a functional construction of a recording/reproduction device 20.

FIG. 18 is a flowchart showing an operation of moving content from the recording/reproduction device 20 to the portable medium 14.

FIG. 19 shows data held in the recording/reproduction device 10 and the portable medium 14, when moving content from the recording/reproduction device 20 to the portable

medium 14.

FIG. 20 is a flowchart showing an operation of moving content from the portable medium 14 to the recording/reproduction device 20.

FIG. 21 shows data held in the recording/reproduction device 20 and the portable medium 14, in a process of moving content from the portable medium 14 to the recording/reproduction device 20.

FIG. 22 shows a construction of a content protection system 3 and a functional construction of a recording/reproduction device 30.

FIG. 23 is a flowchart showing an operation of moving content from the recording/reproduction device 30 to the portable medium 14.

FIG. 24 shows data held in the recording/reproduction device 30 and the portable medium 14, in a process of moving content from the recording/reproduction device 30 to the portable medium 14.

FIG. 25 is a flowchart showing an operation of moving content from the portable medium 14 to the recording/reproduction device 30.

FIG. 26 shows data held in the recording/reproduction device 30 and the portable medium 14, in a process of moving content from the portable medium 14 to the recording/reproduction device 30.

FIG. 27 is a block diagram showing an overall construction of a copyright protection system according to the present invention.

FIG. 28 is a functional block diagram in a fourth ~~first~~ embodiment of the present invention.

FIG. 29 is a flowchart showing an operation of recording content in a recording/reproduction device in the fourth ~~first~~ embodiment of the present invention.

FIG. 30 is a flowchart showing an operation of moving content from the recording/reproduction device to a portable medium in the fourth ~~first~~ embodiment of the present invention.

FIG. 31 shows each data storage state when moving content from the recording/reproduction device to the portable medium in the fourth ~~first~~ embodiment of the present invention.

FIG. 32 shows each data storage state when moving content from the

recording/reproduction device to the portable medium in the fourth ~~first~~ embodiment of the present invention.

FIG. 33 is a flowchart showing an operation of moving content from the portable medium to the recording/reproduction device in the fourth ~~first~~ embodiment of the present invention.

FIG. 34 shows each data storage state when moving content from the portable medium to the recording/reproduction device in the fourth ~~first~~ embodiment of the present invention.

FIG. 35 shows each data storage state when moving content from the portable medium to the recording/reproduction device in the fourth ~~first~~ embodiment of the present invention.

FIG. 36 is a flowchart showing an operation of reproducing content recorded in the recording/reproduction device in the fourth ~~first~~ embodiment of the present invention.

FIG. 37 is a functional block diagram in the fourth ~~first~~ embodiment of the present invention.

FIG. 38 is a flowchart showing an operation of recording content in a recording/reproduction device in a fifth ~~second~~ embodiment of the present invention.

FIG. 39 is a flowchart showing an operation of moving content from the recording/reproduction device to a portable medium in the fifth ~~second~~ embodiment of the present invention.

FIG. 40 shows each data storage state when moving content from the recording/reproduction device to the portable medium in the fifth ~~second~~ embodiment of the present invention.

FIG. 41 shows each data storage state when moving content from the recording/reproduction device to the portable medium in the fifth ~~second~~ embodiment of the present invention.

FIG. 42 is a flowchart showing an operation of moving content from the portable medium to the recording/reproduction device in the fifth ~~second~~ embodiment of the present invention.

FIG. 43 shows each data storage state when moving content from the portable medium to the recording/reproduction device in the fifth ~~second~~ embodiment of the present invention.

FIG. 44 shows each data storage state when moving content from the portable medium to the recording/reproduction device in the fifth ~~second~~ embodiment of the present invention.

FIG. 45 is a flowchart showing an operation of reproducing content recorded in the recording/reproduction device in the fifth ~~second~~ embodiment of the present invention.

Please amend the paragraph [0059] beginning on page 17, as follows:

[0059] (9) Medium Recording Key Storage Unit 109

The medium recording key storage unit 109 receives medium recording key K_T from the medium recording key generation unit 108, and stores received medium recording key K_T. After the write/read unit 113 writes medium recording key K_T to the portable medium 14, the medium recording key storage unit 109 deletes medium recording key K_T stored therein.

(10) Encryption Unit 110

The encryption unit 110 sequentially receives content portions $C4^{(n)}$ from the conversion unit 107. The encryption unit 110 also reads medium ~~device~~ recording key K_T from the medium recording key storage unit 109, and applies encryption algorithm E_2 to each content portion $C4^{(n)}$ using medium recording key K_T as an encryption key, to generate encrypted content portions $EC4^{(n)}$. Which is to say, $EC4^{(n)} = E_2 (C4^{(n)}, K_T)$. Encryption algorithm E_2 used by the encryption unit 110 is AES as one example.

Please amend the paragraph [0089] beginning on page 47, as follows:

[0089] The write/read unit 113 outputs encrypted content portion $EC4^{(n)}$ to the portable medium 14. The input/output unit 132 in the portable medium 14 receives encrypted content portion $EC4^{(n)}$ (step S106). The recording control unit 133 in the portable medium 14 receives encrypted content portion $EC4^{(n)}$ via the input/output unit ~~141~~ 132, and writes encrypted content portion $EC4^{(n)}$ to the encrypted content area 134a in the storage unit 134. The encrypted content area 134a stores encrypted content portion $EC4^{(n)}$ (step S108). As a result of accumulating each encrypted content portion $EC4^{(n)}$ in the encrypted content area 134a, encrypted content EC4 is obtained in the portable medium 14 (step S110).

Please amend the paragraph [0106] beginning on page 47, as follows:

[0106] If the received device ID "ID_A" matches the device ID of the recording/reproduction device 10 (step S136: YES), the encryption/decryption unit 112 reads device unique key Ka from the device unique key storage unit 111, and decrypts encrypted device recording key EK_{HDD}

using device unique key Ka as ~~an encryption key~~ a decryption key, to generate device recording key K_{HDD} (step S138).

The encryption/decryption unit 112 writes generated device recording key K_{HDD} to the device recording key storage unit 102. The device recording key storage unit 102 stores device recording key K_{HDD} (step S139).

Please amend the paragraph [0128] beginning on page 63, as follows:

[0128] (9) Encryption Unit 169

The encryption unit 169 receives content portions $C2^{(n)}$ from the decryption unit 168.

The encryption unit 169 ~~103~~ also reads device recording key K_{PC} from the device recording key storage unit 171. The encryption unit 103 applies encryption algorithm E_1 to each content portion $C2^{(n)}$ using device recording key K_{PC} as an encryption key, to generate encrypted content portions $EC2^{(n)}$. Which is to say, $EC2^{(n)} = E_1 (C2^{(n)}, K_{PC})$.

Please amend the paragraph [0134] beginning on page 66, as follows:

[0134] (14) Display 174 and Speaker 175

The display 174 receives the video signal from the reproduction unit 173, and outputs the video signal. The speaker 175 receives the audio signal from the reproduction unit 173, and outputs the audio signal.

3. Operation of the ~~Operation of the~~ Entire System

The following describes an overall operation of the content protection system 1a and a state of each device in the operation, using flowcharts shown in FIGS. 7 and 14.

Please amend the paragraph [0136] beginning on page 66, as follows:

[0136] The recording/reproduction device 10 remains in the content unusable state (step S14). Also, as a result of moving the content, the portable medium 14 enters the content unusable state (step S15). Meanwhile, the PC 16 to which the content has been moved is in the content usable state (step S16).

The PC 16 ~~recording/reproduction device 10~~ which is in the content usable state outputs and reproduces the content (step S17).

Please amend the paragraph [0148] beginning on page 71, as follows:

[0148] The content provision device 11 and the mobile information terminal 15 have the same functions and constructions as the corresponding devices in the content protection system 1.

Note here that the input/output unit 132, the recording control unit 133, and the device ID area 134d in the portable medium 14 are not shown in FIG. ~~14~~ 17. The portable medium 14 in the content protection system 2 does not have the encrypted device recording key area 134c.

Please amend the paragraph [0159] beginning on page 77, as follows:

[0159] The encryption/decryption unit 2002 encrypts content portion $C4^{(n)}$ using medium recording key K_T as an encryption key, to generate encrypted content portion $EC4^{(n)}$ (step S209). The encryption/decryption unit 2002 outputs generated encrypted content portion $EC4^{(n)}$ to the write/read unit 213.

The write/read unit 213 outputs encrypted content portion $EC4^{(n)}$ to the portable medium 14. The input/output unit 132 in the portable medium 14 receives encrypted content portion $EC4^{(n)}$ (step S210). The recording control unit 133 in the portable medium 14 receives encrypted content portion $EC4^{(n)}$ via the input/output unit ~~141~~ 132, and writes encrypted content portion $EC4^{(n)}$ to the encrypted content area 134a in the storage unit 134. The encrypted content area 134a stores encrypted content portion $EC4^{(n)}$ (step S212).

Please amend the paragraph [0170] beginning on page 81, as follows:

[0170] FIG. 19D shows data held in the recording/reproduction device 20 and the portable medium 14 at a point where the content movement operation ends.

In the recording/reproduction device 20, the storage unit 204 stores encrypted MPEG-2 content EC2, whilst the medium recording key storage unit 209 ~~109~~ and the device recording key storage unit 202 ~~102~~ do not hold any data.

Please amend the paragraph [0181] beginning on page 85, as follows:

[0181] FIG. 21C shows data held in the recording/reproduction device 20 and the portable medium 14 at a point where the content movement operation ends.

In the recording/reproduction device 20, the storage unit 204 stores encrypted MPEG-2 content EC2, the medium recording key storage unit 209 does not hold any data, and the device recording key storage unit 202 ~~102~~ stores device recording key K_{HDD}.

Please amend the paragraph [0182] beginning on page 86, as follows:

[0182] In the portable medium 14, the encrypted content area 134a, the medium recording key area 134b, and the encrypted device recording key area 134c do not hold any data.

At this time, the recording/reproduction device 20 is in the content usable state and can use the MPEG-2 content of a high image quality. Meanwhile, the portable medium 14 does not hold the content and is in the content unusable state.

<Third Embodiment>

The following describes a content protection system 3 as a third embodiment of the present invention.

Please amend the paragraph [0185] beginning on page 87, as follows:

[0185] The content provision device 11 and the mobile information terminal 15 have the same functions and constructions as the corresponding devices in the content protection system 1.

Note here that the input/output unit 132, the recording control unit 133, and the device ID area 134d in the portable medium 14 are not shown in FIG. ~~14~~ 22. The portable medium 14 in the content protection system 3 does not have the medium recording key area 134b and the encrypted device recording key area 134c, but has a content key area 3002.

Please amend the paragraph [0197] beginning on page 92, as follows:

[0197] In the recording/reproduction device 30, the storage unit 304 stores encrypted MPEG-2 content EC2, and the content key storage unit 3001 stores content key K_C.

In the portable medium 14, meanwhile, the encrypted content key 134a and the content key area 3002 do not hold any data.

At this time, the recording/reproduction device 30 ~~20~~ is in the content usable state and can use the MPEG-2 content. On the other hand, the portable medium 14 does not hold the content and is in the content unusable state.

Please amend the paragraph [0201] beginning on page 94, as follows:

[0201] 3. Operation of Transferring the Content Use Right from the Portable Medium 14 to the Recording/reproduction Device 30

FIG. 25 is a flowchart showing an operation of moving content from the portable medium 14 to the recording/reproduction device 30. This operation is a detailed operation of step S7 in FIG. 7 where "recording/reproduction device 10" has been replaced with "recording/reproduction device 30".

The recording control unit 133 in the portable medium 14 deletes encrypted content EC4 from the encrypted content area 134a (step S331). The recording control unit 133 then reads content key K_C from the content key area 3002 (step S332), and the device ID "ID_A" from the predetermined area (step S333~~S332~~).

Please amend the paragraph [0207] beginning on page 96, as follows:

[0207] In the recording/reproduction device 30, the storage unit 304 stores encrypted MPEG-2 content EC2, and the content key storage unit 3001 stores content key K_C.

In the portable medium 14, the encrypted content area 134a and the content key area 3002 do not hold any data.

At this time, the recording/reproduction device 30 ~~10~~ is in the content usable state and can use the MPEG-2 content of a high image quality. On the other hand, the portable medium 14 does not hold the content and so is in the content unusable state.

<Fourth Embodiment>

The following describes another embodiment of the present invention with reference to drawings. FIG. 27 is a block diagram showing an overall construction of a copyright protection system to which the present invention relates. This system is roughly made up of a content provision device 1101 for providing content, a recording/reproduction device 1102 for acquiring the content, recording/reproducing the content, and moving the content, and a recording/reproduction device 1103 and a portable medium 1104 for acquiring the moved content.

Please amend the paragraph [0218] beginning on page 104, as follows:

[0218] Step S402: The authentication unit 1223 in the recording/reproduction device 1102 ~~104~~

performs mutual authentication with the authentication unit 1224 in the portable medium 1104. If the mutual authentication is successful, the authentication units 1223 and 1224 each generate a session key. If the mutual authentication is not successful, the operation is terminated.

Step S403: The write/read unit 1213 reads the copy control information stored in the copy control information storage unit 1204 and the content key stored in the content key storage unit 1206.

Please amend the paragraph [0221] beginning on page 105, as follows:

[0221]Step S408: The second encrypted content stored in the encrypted content storage unit 1211 is deleted.

FIGS. 31 and 32 ~~30 and 31~~ show data storage states of the recording/reproduction device 1102 and the portable medium 1104 in the above operation. FIGS. 31A ~~30A~~ shows data storage states when step S401 begins, FIG. 31B ~~30B~~ shows data storage states when step S403 ends, FIG. 31C ~~30C~~ shows data storage states when step S404 ends, FIG. 31D ~~30D~~ shows data storage states when step S405 ends, FIG. 32E ~~31E~~ shows data storage states when step S407 ends, and FIG. 32F ~~31F~~ shows data storage states when step S408 ends.

Please amend the paragraph [0222] beginning on page 105, as follows:

[0222] In step S403, the control unit 1203 makes the content key stored in the content key storage unit 1206 unusable so as to prohibit subsequent access to the stored content key. As a result, even if power fails or the portable medium 1104 is removed from the recording/reproduction device 1102 by unauthorized means at a point between when step S404 ends and when step S405 begins (FIG. ~~30C~~ 31C), a situation where the content key is simultaneously usable in both the recording/reproduction device 1102 and the portable medium 1104 can be avoided. Also, even if power fails at any point from FIGS. 31A to 32F~~30A to 31F~~, the content key exists in any of the recording/reproduction device 1102 and the portable medium 1104, and so a situation where the content key is lost in both the move source and the move destination and as a result the content becomes unusable can be avoided.

Please amend the paragraph [0223] beginning on page 106, as follows:

[0223] The mutual authentication and session key sharing performed by the authentication units

1223 and 1224 in step S402 can be realized using, for example, a challenge-response mutual authentication and session key sharing method. The challenge-response mutual authentication and session key sharing method is well known and so its explanation has been omitted here.

An operation of moving content from the portable medium 1104 to the recording/reproduction device 1102 is described below, with reference to FIG. ~~32~~ 33.

Please amend the paragraph [0225] beginning on page 107, as follows:

[0225] Step S602: The authentication unit 1223 in the recording/reproduction device 1102 ~~104~~ performs mutual authentication with the authentication unit 1224 in the portable medium 1104. If the mutual authentication is successful, the authentication units 1223 and 1224 each generate a session key. If the mutual authentication is not successful, the operation is terminated.

Step S603: The write/read unit 1213 reads the copy control information stored in the copy control information storage unit 1216 and the content key stored in the content key storage unit 1217 in the portable medium 1104. Here, the encryption/decryption unit 1226 in the portable medium 1104 encrypts the copy control information and the content key using the session key, and outputs the encrypted copy control information and content key to the recording/reproduction device 1102. The encryption/decryption unit 1225 in the recording/reproduction device 1102 decrypts the received encrypted copy control information and content key using the session key, and outputs the decrypted copy control information and content key to the write/read unit 1213.

Please amend the paragraph [0226] beginning on page 108, as follows:

[0226] Step S604: The write/read unit 1213 stores the copy control information and the content key respectively to the copy control information storage unit 1204 and the content key storage unit 1206 in the recording/reproduction device 1102. At this time, the control unit 1203 ~~223~~ makes the content key stored in the content key storage unit 1206 unusable so as to prohibit access to the stored content key.

Step S605: The portable medium 1104 deletes the copy control information stored in the copy control information storage unit 1216 and the content key stored in the content key storage unit 1217.

Please amend the paragraph [0227] beginning on page 108, as follows:

[0227] The control unit 1203 ~~223~~ makes the content key stored in the content key storage unit 1206 usable so as to permit access to the stored content key.

Step S606: The write/read unit 1213 reads the second encrypted content stored in the encrypted content storage unit 1218 in the portable medium 1104.

Step S607: The read second encrypted content is stored to the encrypted content storage unit 1211 in the recording/reproduction device 1102.

Please amend the paragraph [0228] beginning on page 108, as follows:

[0228] Step S608: The second encrypted content stored in the encrypted content storage unit 1218 in the portable medium 1104 is deleted.

FIGS. 34 and 35 ~~33 and 34~~ show data storage states of the recording/reproduction device 1102 and the portable medium 1104 in the above operation. FIG. 34A ~~33A~~ shows data storage states when step S601 begins, FIG. 34B ~~33B~~ shows data storage states when step S604 ends, FIG. 34C ~~33C~~ shows data storage states when step S605 ends, FIG. 34D ~~33D~~ shows data storage states when step S607 ends, and FIG. 35E ~~34E~~ shows data storage states when step S608 ends.

Please amend the paragraph [0229] beginning on page 109, as follows:

[0229] An operation of reproducing the recorded first encrypted content or second encrypted content in the recording/reproduction device 1102 is described next, with reference to FIG. ~~35~~ 36.

Step S801: The decryption unit 1221 reads the first encrypted content from the encrypted content storage unit 1210 or the second encrypted content from the encrypted content storage unit 1211.

Please amend the paragraph [0234] beginning on page 111, as follows:

[0234] Step S402: The authentication unit 1223 in the recording/reproduction device 1102 ~~104~~ performs mutual authentication with the authentication unit 1224 in the portable medium 1104. If the mutual authentication is successful, the authentication units 1223 and 1224 each generate a session key. If the mutual authentication is not successful, the operation is terminated.

Step S403: The write/read unit 1213 reads the copy control information stored in the

copy control information storage unit 1204 and the content key stored in the content key storage unit 1206.

Please amend the paragraph [0239] beginning on page 113, as follows:

[0239] The fourth embodiment describes the case where the control unit 1203 is provided in the recording/reproduction device 1102, but a control unit may be provided in both the recording/reproduction device 1102 and the portable medium 1104.

The fourth embodiment describes a construction in which the received content and the converted content are each encrypted using the same content key, but the present invention is not limited to this construction. For example, the received content and the converted content may be encrypted using different content keys. The following describes this construction as a fifth embodiment of the present invention.

<Fifth Embodiment>

FIG. 37 ~~36~~ is a functional block diagram showing a recording/reproduction device 1102a and a portable medium 1104a when content is recorded and reproduced by the recording/reproduction device 1102a and further moved from the recording/reproduction device 1102a to the portable medium 1104a.

Please amend the paragraph [0241] beginning on page 114, as follows:

[0241] The recording/reproduction device 1102a further includes an encrypted content storage unit 1211a, a decryption unit 1221a, a reproduction unit 1222a, a judgment unit 1212a, an authentication unit ~~units~~ 1223a ~~and 1224a~~, an encryption/decryption unit ~~units~~ 1225a ~~and 1226a~~, and a write/read unit 1213a. The encrypted content storage unit 1211a stores the second encrypted content. The decryption unit 1221a decrypts the first encrypted content using the first content key or the second encrypted content using the second content key. The reproduction unit 1222a reproduces the decrypted first encrypted content or second encrypted content. The judgment unit 1212a judges whether the second encrypted content stored in the encrypted content storage unit 1211a is movable from the recording/reproduction device 1102a to the portable medium 1104a based on the copy control information stored in the copy control information storage unit 1204a, or judges whether the second encrypted content stored in an encrypted content storage unit 1218a of the portable medium 1104a is movable from the portable

medium 1104a to the recording/reproduction device 1102a based on the copy control information stored in a copy control information storage unit 1216a of the portable medium 1104 described later. The authentication unit 1223a performs mutual authentication between the recording/reproduction device 1102a and the portable medium 1104a. The encryption/decryption unit 1225a encrypts/decrypts the copy control information and the first or second content key to be transferred between the recording/reproduction device 1102a and the portable medium 1104a when the authentication is successful. The write/read unit 1213a writes the copy control information stored in the copy control information storage unit 1204a, the first content key stored in the content key storage unit 1206a1 or the second content key stored in the content key storage unit 1206a2, and the second encrypted content stored in the encrypted content storage unit 1211a to the portable medium 1104a, or reads data from the portable medium 1104a.

Please amend the paragraph [0245] beginning on page 117, as follows:

[0245] An operation of recording received content in the recording/reproduction device 1102a is described below, with reference to FIG. ~~37~~ 38.

Step S501a: The reception unit 1201a in the recording/reproduction device 1102a receives content and copy control information.

Step S502a: The judgment unit 1202a judges whether the copy control information indicates that the received content is recordable to the recording/reproduction device 1102a. If the judgment unit 1202a judges that the received content is not recordable, the operation is terminated. If the judgment unit 1202a judges that the received content is recordable, the operation is continued.

Please amend the paragraph [0249] beginning on page 119, as follows:

[0249] Also, for example when the received content is MPEG-2 video content, the conversion unit 1207a converts the received content to MPEG-4 video content.

An operation of moving content from the recording/reproduction device 1102a to the portable medium 1104a is described next, with reference to FIG. ~~38~~ 39.

Step S401a: The judgment unit 1212a in the recording/reproduction device 1102a receives the copy control information stored in the copy control information storage unit 1204a via the write/read unit 1213a, and judges whether the received copy control information indicates

that the second encrypted content stored in the encrypted content storage unit 1211a is movable to the portable medium 1104a. If the judgment unit 1212a judges that the second encrypted content is not movable, the operation is terminated. If the judgment unit 1212a judges that the second encrypted content is movable, the operation is continued.

Please amend the paragraph [0250] beginning on page 120, as follows:

[0250] Step S402a: The authentication unit 1223a in the recording/reproduction device 1102a ~~104a~~ performs mutual authentication with the authentication unit 1224a in the portable medium 1104a. If the mutual authentication is successful, the authentication units 1223a and 1224a each generate a session key. If the mutual authentication is not successful, the operation is terminated.

Step S403a: The write/read unit 1213a reads the copy control information stored in the copy control information storage unit 1204a and the second content key stored in the content key storage unit 1206a2.

Please amend the paragraph [0251] beginning on page 120, as follows:

[0251] At this time, the control unit 1203a makes the first content key stored in the content key storage unit 1206a1 and the second content key stored in the content key storage unit 1206a2 unusable, so as to prohibit subsequent access to the stored first and second content keys.

Step S404a: The write/read unit 1213a encrypts the read copy control information and second content key using the session key through the encryption/decryption unit 1225a, and transmits the encrypted copy control information and second content key to the portable medium 1104a. The portable medium 1104a decrypts the received encrypted copy control information and second content key using the session key through the encryption/decryption unit 1226a, and stores the decrypted copy control information and second content key therein.

Please amend the paragraph [0253] beginning on page 121, as follows:

[0253] Step S408a: The second encrypted content stored in the encrypted content storage unit 1211a is deleted.

FIGS. 40 and 41 ~~39 and 40~~ show data storage states of the recording/reproduction device 1102a and the portable medium 1104a in the above operation. FIGS. 40A ~~39A~~ shows data storage states when step S401a begins, FIG. 40B ~~39B~~ shows data storage states when step S403a

ends, FIG. 40C ~~39C~~ shows data storage states when step S404a ends, FIG. 40D ~~39D~~ shows data storage states when step S405a ends, FIG. 41E ~~40E~~ shows data storage states when step S407a ends, and FIG. 41F ~~40F~~ shows data storage states when step S408a ends.

Please amend the paragraph [0254] beginning on page 122, as follows:

[0254] In step S403a, the control unit 1203a makes the first content key stored in the content key storage unit 1206a1 and the second content key stored in the content key storage unit 1206a2 unusable, so as to prohibit subsequent access to the stored first and second content keys. As a result, even if power fails or the portable medium 1104a is removed from the recording/reproduction device 1102a by unauthorized means at a point between when step S404a ends and step S405a begins, a situation where the first and second content keys are usable simultaneously in both the recording/reproduction device 1102a and the portable medium 1104a can be avoided. Also, even if power fails at any point from FIGS. 40A to 41F ~~39A to 40F~~, the first and second content keys exist in any of the recording/reproduction device 1102a and the portable medium 1104a, and so a situation where the first and second content keys are lost in both the move source and the move destination and as a result the content becomes unusable can be avoided.

Please amend the paragraph [0255] beginning on page 122, as follows:

[0255] The mutual authentication and session key sharing performed by the authentication units 1223a and 1224a in step S402a can be realized using, for example, a challenge-response mutual authentication and session key sharing method as in the fourth embodiment. The challenge-response mutual authentication and session key sharing method is well known and so its explanation has been omitted here.

An operation of moving content form the portable medium 1104a to the recording/reproduction device 1102a is described below, with reference to FIG. ~~41~~ 42.

Please amend the paragraph [0257] beginning on page 123, as follows:

[0257] Step S602a: The authentication unit 1223a in the recording/reproduction device 1102a ~~104a~~ performs mutual authentication with the authentication unit 1224a in the portable medium 1104a. If the mutual authentication is successful, the authentication units 1223a and 1224a each

generate a session key. If the mutual authentication is not successful, the operation is terminated.

Step S603a: The write/read unit 1213a reads the copy control information stored in the copy control information storage unit 1216a and the second content key stored in the content key storage unit 1217a in the portable medium 1104a. Here, the encryption/decryption unit 1226a in the portable medium 1104a encrypts the copy control information and the second content key using the session key, and outputs the encrypted copy control information and second content key to the recording/reproduction device 1102a. The encryption/decryption unit 1225a in the recording/reproduction device 1102a decrypts the received encrypted copy control information and second content key using the session key, and outputs the decrypted copy control information and second content key to the write/read unit 1213a.

Please amend the paragraph [0259] beginning on page 124, as follows:

[0259] Step S605a: The copy control information stored in the copy control information storage unit 1216a and the second content key stored in the content key storage unit 1217a are deleted.

The control unit 1203a makes the second content key stored in the content key storage unit 1206a2 and the first content key stored in the content key storage unit 1206a1 usable.

Please amend the paragraph [0261] beginning on page 125, as follows:

[0261] FIGS. 43 and 44 ~~42 and 43~~ show data storage states of the recording/reproduction device 1102a and the portable medium 1104a in the above operation. FIG. 43A ~~42A~~ shows data storage states when step S601a begins, FIG. 43B ~~42B~~ shows data storage states when step S604a ends, FIG. 43C ~~42C~~ shows data storage states when step S605a ends, FIG. 43D ~~42D~~ shows data storage states when step S607a ends, and FIG. 44E ~~43E~~ shows data storage states when step S608a ends.

Please amend the paragraph [0262] beginning on page 125, as follows:

[0262] An operation of reproducing the recorded first encrypted content or second encrypted content in the recording/reproduction device 1102a is described next, with reference to FIG. ~~44~~ 45.

Step S701a: The decryption unit 1221a reads the first encrypted content from the encrypted content storage unit 1210a or the second encrypted content from the encrypted content storage unit 1211a.

Please amend the paragraph [0265] beginning on page 126, as follows:

[0265] Since the control unit 1203a makes the first and second content keys unusable so as to prohibit access to the first and second content keys in step S702a, it is possible to prevent the decryption and reproduction of the first encrypted content and the decryption and reproduction of the second encrypted content from being simultaneously performed.

<Modifications>

(1) In the fourth and fifth embodiments, the provision of content from the content provision device 1101 ~~or 1101a~~ to the recording/reproduction device 1102 or 1102a can be conducted using various methods such as terrestrial broadcasting, satellite broadcasting, internet communications, and recording media such as DVD.

Please amend the paragraph [0282] beginning on page 136, as follows:

[0282] (12) Also, the present invention is a recording/reproduction device capable of moving content to a portable medium or moving the content from the portable medium, including: a content storage unit operable to store first encrypted content and second encrypted content that is related to the first encrypted content; a key storage unit operable to store a content key for decrypting the first encrypted content or the second encrypted content; and a key control unit operable to control access to the content key, wherein when moving the first encrypted content or the second encrypted content from the recording/reproduction device to the portable medium, the content key stored in the key storage unit in the recording/reproduction device is stored to the portable medium and the first encrypted content or the second encrypted content stored in the content storage unit in the recording/reproduction ~~first~~ device is stored to the portable medium under the control of the key control unit in the recording/reproduction device.

Please amend the paragraph [0291] beginning on page 140, as follows:

[0291](3) The present invention includes not only the case of moving the content which has undergone the image conversion, but also the case of moving the content without the image conversion. Which is to say, the present invention is a terminal device that transfers a right to use content to a portable medium while protecting a copyright of the content, including: a storage unit storing first encrypted content generated by encrypting the content, a device key for

decrypting the first encrypted content, and a medium key different from the device key; a decryption unit operable to decrypt the first encrypted content using the device key to generate the content; an encryption unit operable to encrypt the generated content using the medium key to generate second encrypted content; a write unit operable to write the device key, the medium key, and the second encrypted content to the portable medium; and a key deletion unit operable to delete the device key from the ~~first~~ storage unit.